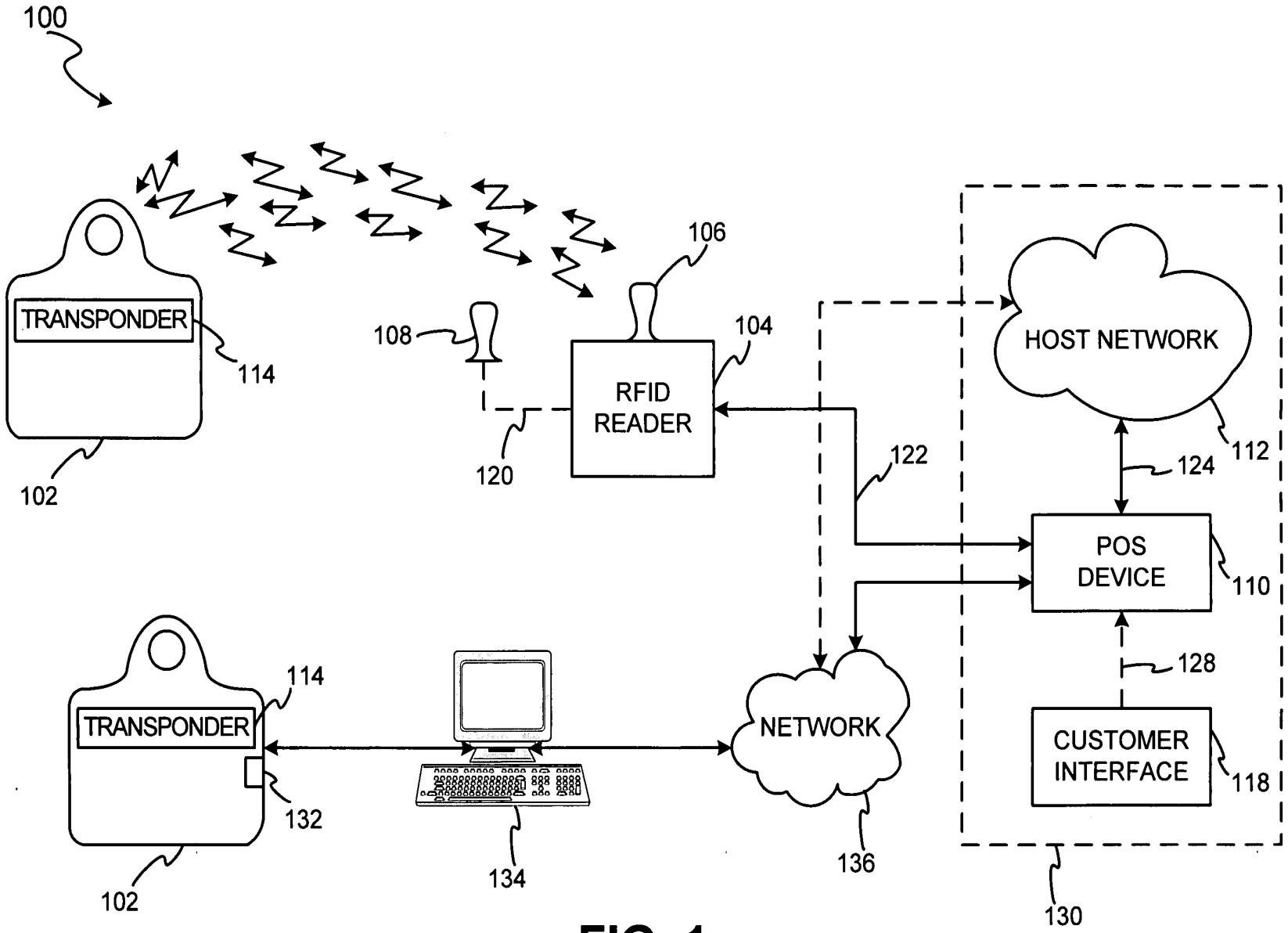
100
TRANSPONDER
114
102
108
106
104
RFID
READER
120
122
HOST NETWORK
112
124
POS
DEVICE
110
128
CUSTOMER
INTERFACE
118
130
TRANSPONDER
114
132
102
134
NETWORK
136

FIG. 1

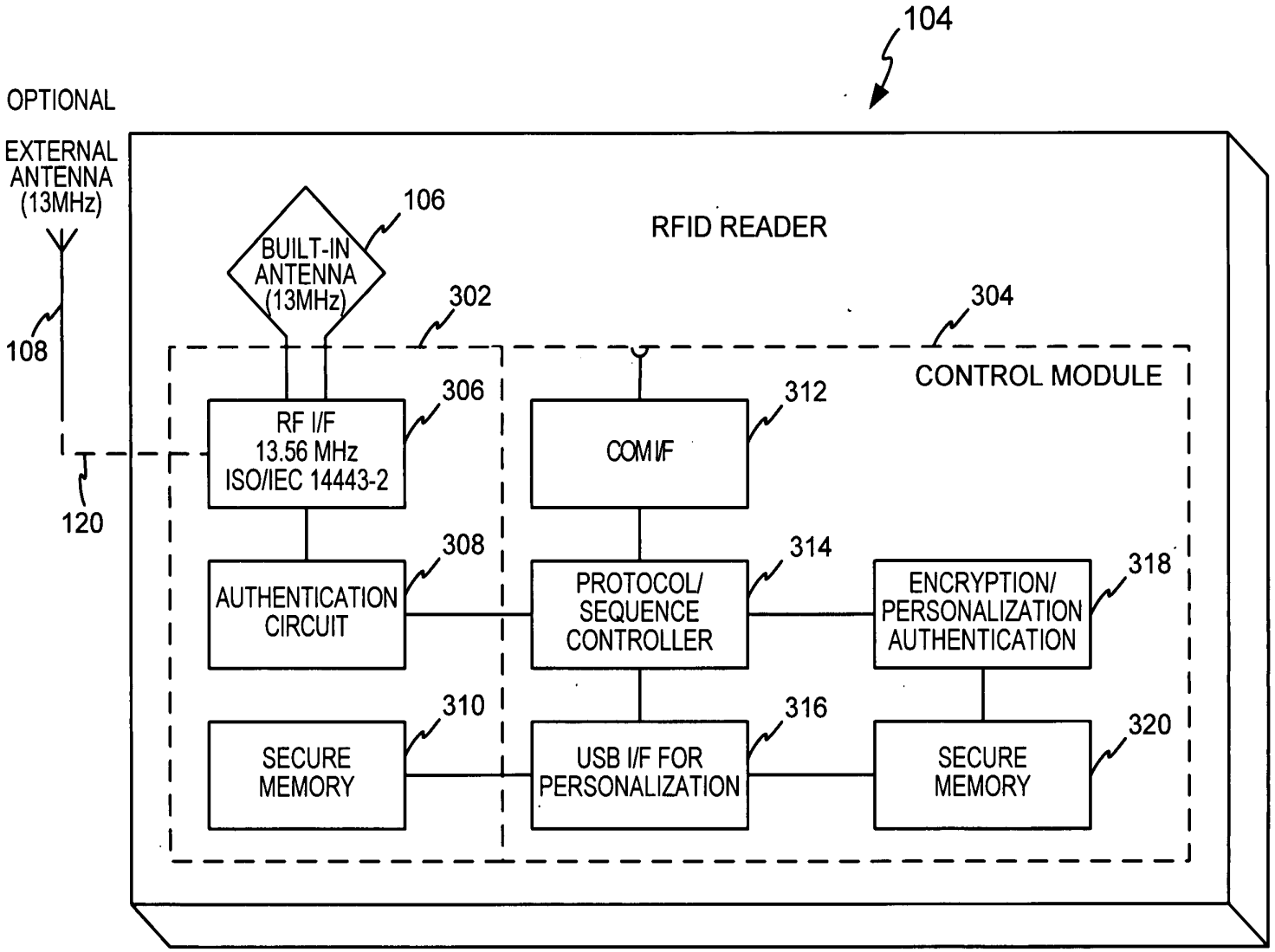
104
OPTIONAL
EXTERNAL ANTENNA (13MHz)
108
120
BUILT-IN ANTENNA (13MHz)
106
RFID READER
302
304
CONTROL MODULE
RF I/F 13.56 MHz ISO/IEC 14443-2
306
COM I/F
312
AUTHENTICATION CIRCUIT
308
PROTOCOL/ SEQUENCE CONTROLLER
314
ENCRYPTION/ PERSONALIZATION AUTHENTICATION
318
SECURE MEMORY
310
USB I/F FOR PERSONALIZATION
316
SECURE MEMORY
320

FIG. 3

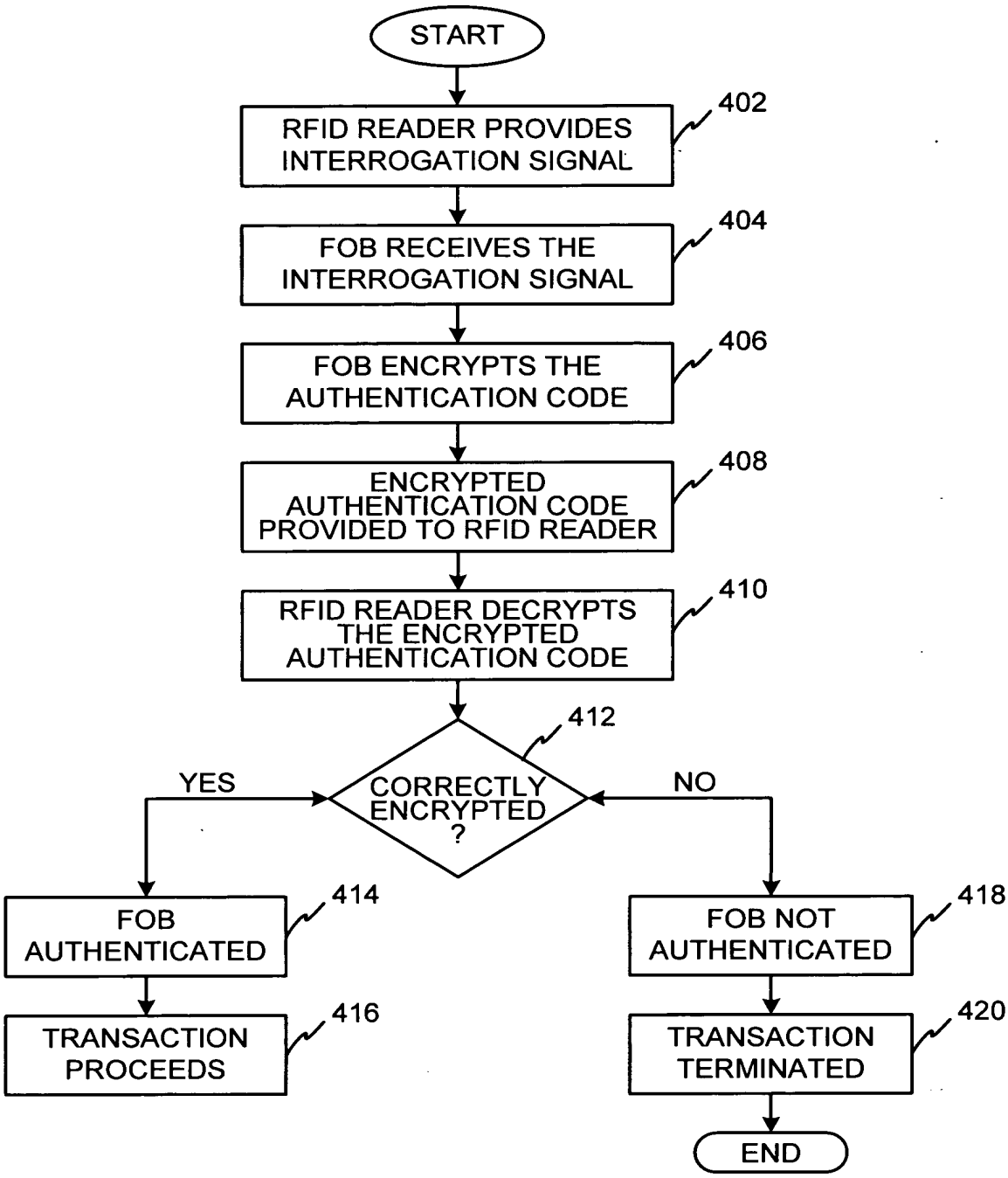
START
RFID READER PROVIDES INTERROGATION SIGNAL
402
FOB RECEIVES THE INTERROGATION SIGNAL
404
FOB ENCRYPTS THE AUTHENTICATION CODE
406
ENCRYPTED AUTHENTICATION CODE PROVIDED TO RFID READER
408
RFID READER DECRYPTS THE ENCRYPTED AUTHENTICATION CODE
410
CORRECTLY ENCRYPTED ?
412
YES
NO
FOB AUTHENTICATED
414
TRANSACTION PROCEEDS
416
FOB NOT AUTHENTICATED
418
TRANSACTION TERMINATED
420
END

FIG. 4

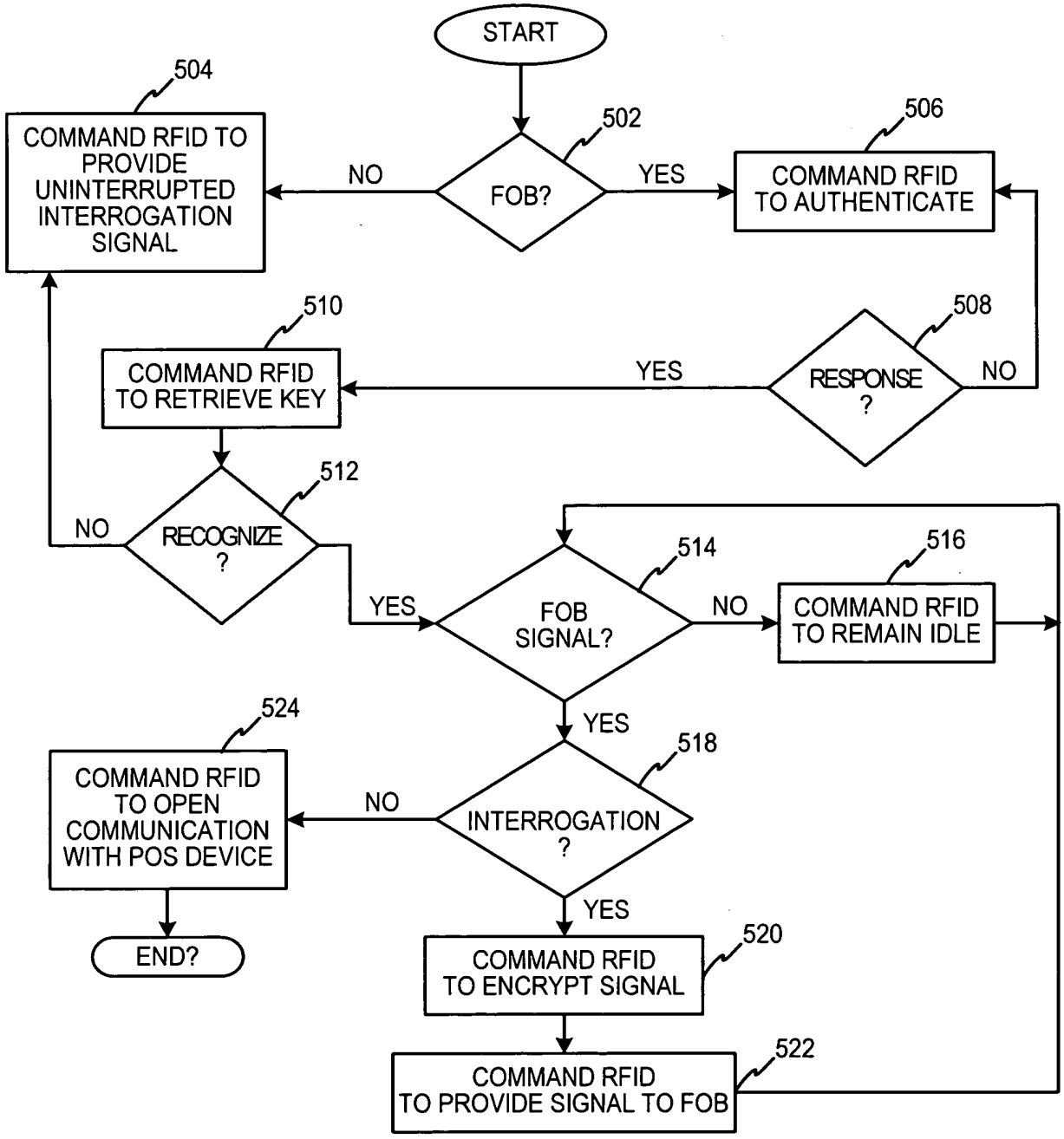
START
502
FOB?
NO
YES
504
COMMAND RFID TO PROVIDE UNINTERRUPTED INTERROGATION SIGNAL
506
COMMAND RFID TO AUTHENTICATE
508
RESPONSE ?
YES
NO
510
COMMAND RFID TO RETRIEVE KEY
512
RECOGNIZE ?
NO
YES
514
FOB SIGNAL?
NO
516
COMMAND RFID TO REMAIN IDLE
YES
518
INTERROGATION ?
NO
524
COMMAND RFID TO OPEN COMMUNICATION WITH POS DEVICE
END?
YES
520
COMMAND RFID TO ENCRYPT SIGNAL
522
COMMAND RFID TO PROVIDE SIGNAL TO FOB

FIG. 5

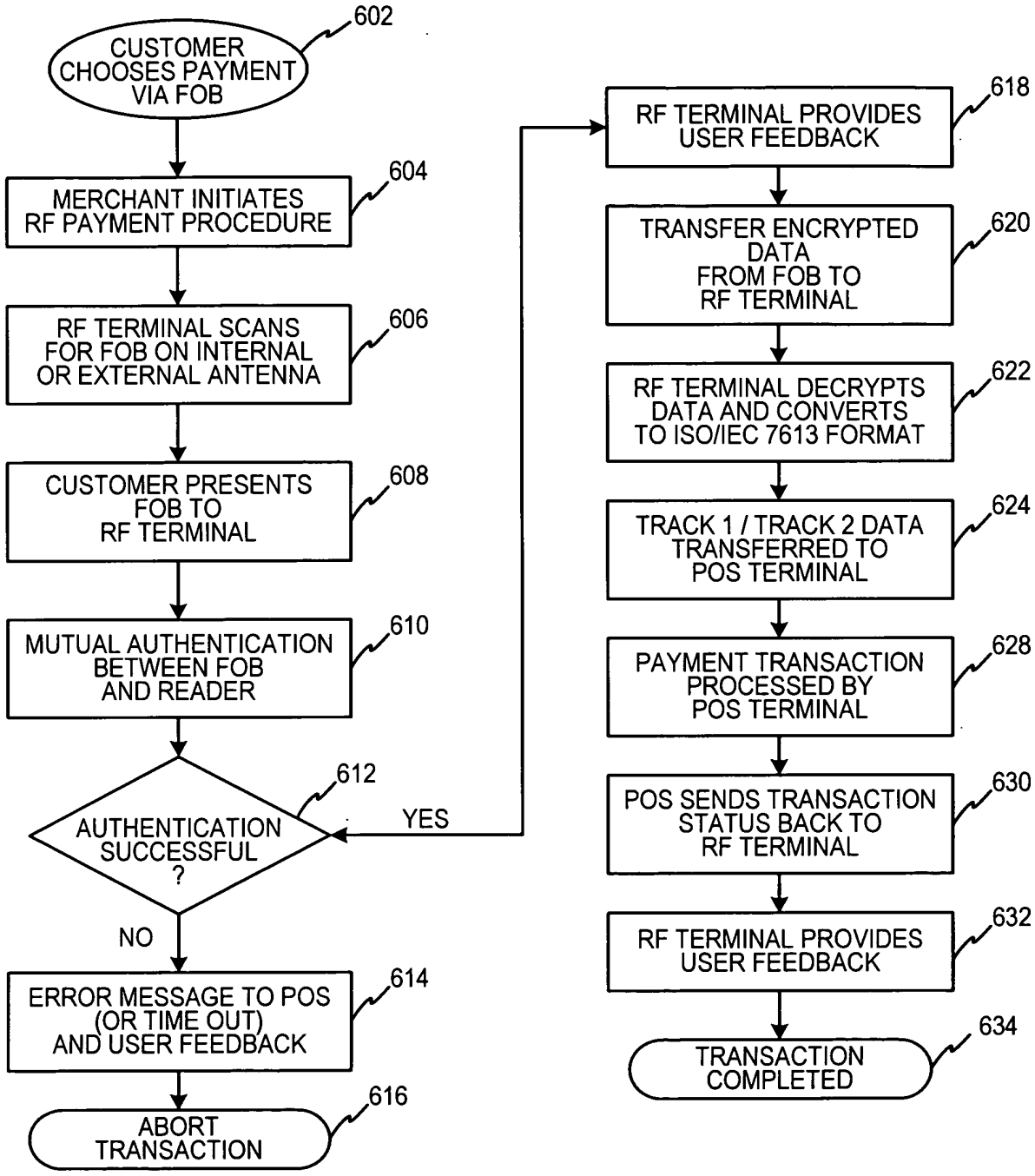
602
CUSTOMER CHOOSES PAYMENT VIA FOB
604
MERCHANT INITIATES RF PAYMENT PROCEDURE
606
RF TERMINAL SCANS FOR FOB ON INTERNAL OR EXTERNAL ANTENNA
608
CUSTOMER PRESENTS FOB TO RF TERMINAL
610
MUTUAL AUTHENTICATION BETWEEN FOB AND READER
612
AUTHENTICATION SUCCESSFUL ?
YES
NO
614
ERROR MESSAGE TO POS (OR TIME OUT) AND USER FEEDBACK
616
ABORT TRANSACTION
618
RF TERMINAL PROVIDES USER FEEDBACK
620
TRANSFER ENCRYPTED DATA FROM FOB TO RF TERMINAL
622
RF TERMINAL DECRYPTS DATA AND CONVERTS TO ISO/IEC 7613 FORMAT
624
TRACK 1 / TRACK 2 DATA TRANSFERRED TO POS TERMINAL
628
PAYMENT TRANSACTION PROCESSED BY POS TERMINAL
630
POS SENDS TRANSACTION STATUS BACK TO RF TERMINAL
632
RF TERMINAL PROVIDES USER FEEDBACK
634
TRANSACTION COMPLETED

FIG. 6

*** Track 1 Layout: *** | SS | FC | PAN | Name | FS | Additional Data | ES | LRC |

FIG. 7

*** Track 2 Layout: *** | SS | PAN | FS | Additional Data | ES | LRC |

FIG. 8

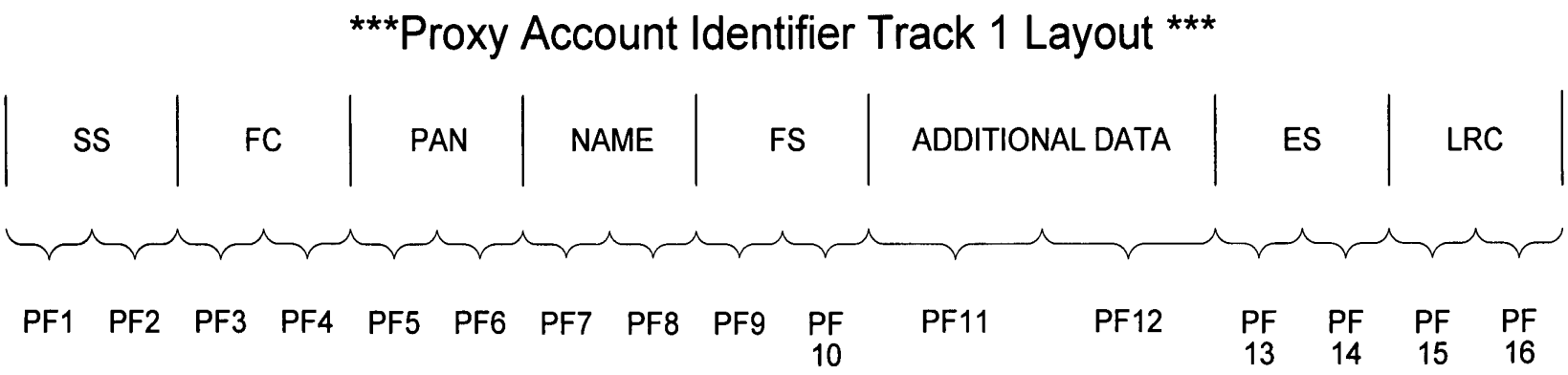
***Proxy Account Identifier Track 1 Layout ***
SS
FC
PAN
NAME
FS
ADDITIONAL DATA
ES
LRC
PF1
PF2
PF3
PF4
PF5
PF6
PF7
PF8
PF9
PF 10
PF11
PF12
PF 13
PF 14
PF 15
PF 16

FIG. 9

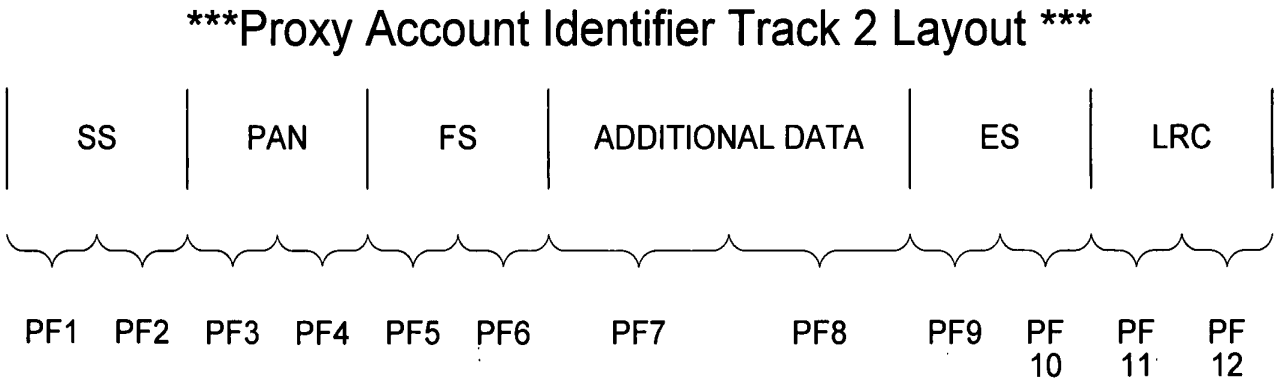
***Proxy Account Identifier Track 2 Layout ***
SS
PAN
FS
ADDITIONAL DATA
ES
LRC
PF1
PF2
PF3
PF4
PF5
PF6
PF7
PF8
PF9
PF 10
PF 11
PF 12

FIG. 10

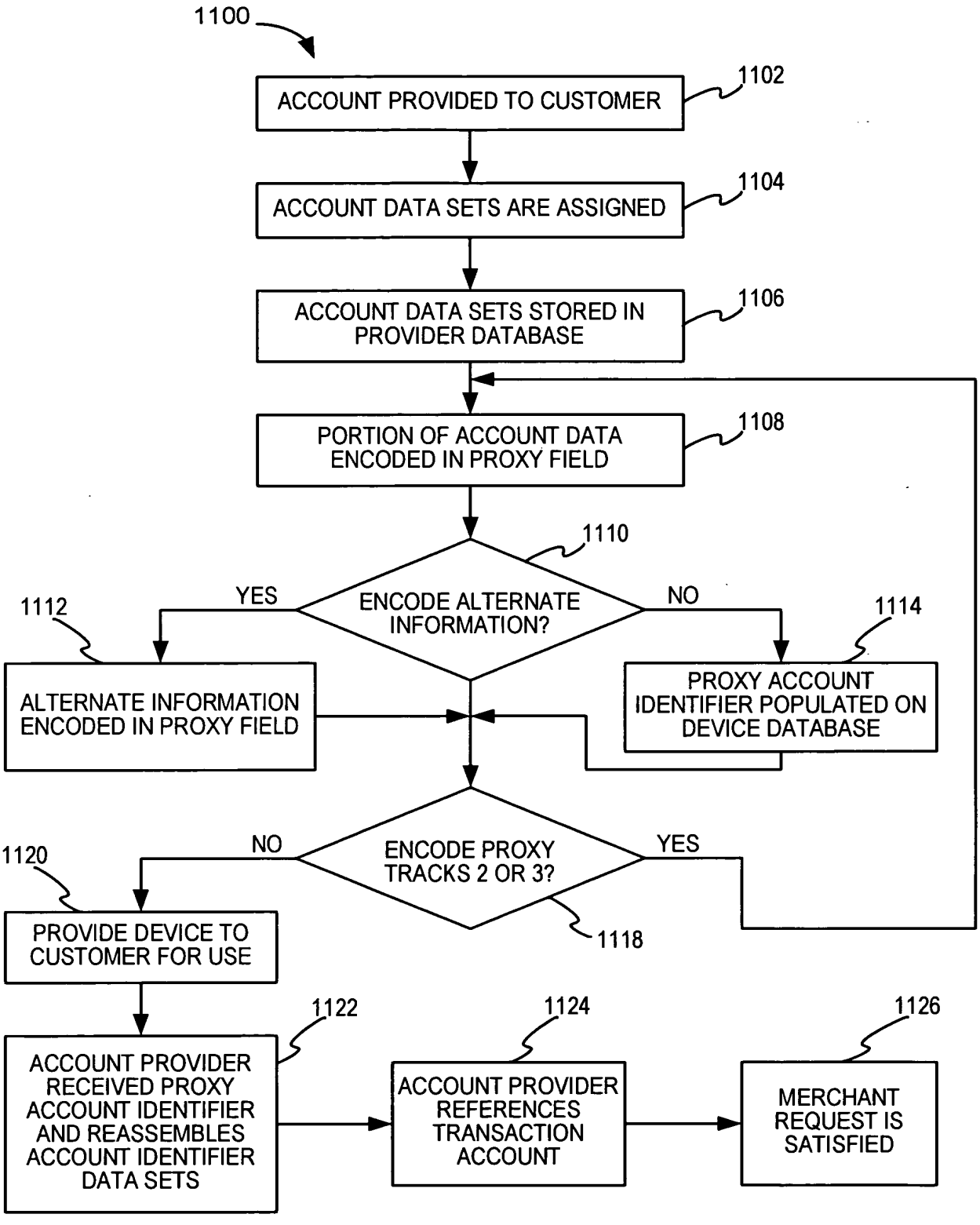
1100
ACCOUNT PROVIDED TO CUSTOMER
1102
ACCOUNT DATA SETS ARE ASSIGNED
1104
ACCOUNT DATA SETS STORED IN PROVIDER DATABASE
1106
PORTION OF ACCOUNT DATA ENCODED IN PROXY FIELD
1108
ENCODE ALTERNATE INFORMATION?
1110
YES
NO
1112
ALTERNATE INFORMATION ENCODED IN PROXY FIELD
1114
PROXY ACCOUNT IDENTIFIER POPULATED ON DEVICE DATABASE
ENCODE PROXY TRACKS 2 OR 3?
1118
NO
YES
1120
PROVIDE DEVICE TO CUSTOMER FOR USE
ACCOUNT PROVIDER RECEIVED PROXY ACCOUNT IDENTIFIER AND REASSEMBLES ACCOUNT IDENTIFIER DATA SETS
1122
ACCOUNT PROVIDER REFERENCES TRANSACTION ACCOUNT
1124
MERCHANT REQUEST IS SATISFIED
1126

FIG. 11

MasterCard Track Layout in Track 2

SS	PAN	FS	ADDITIONAL DATA	ES	LRC

;3111222233334444=99121010000000000?

FIG. 12

MasterCard Proxy Account Identifier Track Layout in Track 2

SS	PAN	FS	ADDITIONAL DATA	ES	LRC

;31114444********=92**101000000000000?

PF3 PF5 PF 7 PF 8

FIG. 13